[6] C. Hooley, *On Artin's conjecture*, J. für Math., Band 225, 1967, pp. 209–220.
[7] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, B. G. Teubner, Leipzig und Berlin 1918.
[8] — *Vorlesungen über Zahlentheorie*, Dritter Band, Hirzel, Leipzig 1927.
[9] S. Lang, *Algebra*, Addison–Wesley, 1967.
[10] W. Ledermann, *The Theory of Finite Groups*, Oliver and Boyd, 1957.
[11] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.
[12] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) 21 (1922), pp. 235–255.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF QUEENSLAND
Brisbane, Queensland, Australia

Received on 21. 2. 1974 (537)

ACTA ARITHMETICA
XXIX (1976)

Conjugate algebraic numbers on circles

by

VEIKKO ENNOLA and C. J. SMYTH (Turku)

1. Introduction. In 1969, R. M. Robinson [4] posed the following question:

(I) Which circles $|z-\gamma| = R$ contain infinitely many sets of conjugate algebraic integers?

In order to answer this question, we have asked, more generally:

(II) Which algebraic numbers have all their conjugates lying on a circle?

In this paper we give a complete answer to the second question (Theorems 2 and 3). We also find all circles which contain infinitely many sets of conjugate algebraic numbers. This enables us to show, towards answering question (I), that the following holds:

THEOREM 1. *For every $n \geqslant 1$ there are algebraic numbers γ of degree n such that there is a circle of centre γ containing infinitely many sets of conjugate algebraic integers.*

There is a method which should, in principle, enable one, from Theorem 3, to give a complete answer to (I), but so far we have only worked out the details when γ is of degree at most 4.

Previous partial answers to (I) and (II) have been as follows: Robinson [4] answered (I), under the assumption that γ is rational. Question (II) is very easy when the centre γ is rational — see [2], Theorem 3. In [1] the first author answered both (I) and (II) when γ is totally real, and in [2] we did the same for γ not totally real and of degree 3 or 4.

When considering (I) and (II), we can, because of the above results, consider only circles with irrational centre. Hence, since any rational or quadratic β lies, with its other conjugate (if any), on a circle of rational centre (of course they lie on many circles), such β can be excluded from consideration in answering question (II). Further, these β are clearly of no interest to question (I). We can therefore confine our attention to the set $\mathscr{B}$ of all algebraic numbers β, of degree at least 3 over the rationals Q, whose conjugates (including β) all lie on a circle with irrational centre $\gamma(\beta)$. It is easy to see that $\gamma(\beta)$ must be a real algebraic number.

For convenience, we divide $\mathscr{B}$ into disjoint subsets, which we treat separately:

$\mathscr{B}_* = \{\beta \in \mathscr{B} |$ some conjugate of β is real$\}$,

$\mathscr{B}_{tr} = \{\beta \in \mathscr{B} |\ \beta$ totally imaginary, $\gamma(\beta)$ totally real$\}$,

and, for each $n \geqslant 3$,

$\mathscr{B}_n = \{\beta \in \mathscr{B} |\ \beta$ totally imaginary, $\gamma(\beta)$ of degree n and not totally real$\}$.

We have

$$\mathscr{B} = \mathscr{B}_* \cup \mathscr{B}_{tr} \cup \Big(\bigcup_{n=3}^{\infty} \mathscr{B}_n\Big).$$

The set $\mathscr{B}_{tr}$ has been characterized in [1]; $\mathscr{B}_*$ and $\mathscr{B}_n$ are given by Theorems 2 and 3, respectively.

2. Statement of results. The letters s, b, c will denote rational numbers such that $c^2 > 4b$. We let $\varrho_1 < \varrho_2$ be the real roots of $x^2 + cx + b = 0$. Put $K = Q(\varrho_1)$, so that $[K:Q] = 1$ or 2. We take n to be an integer $\geqslant 3$, and define

$$\xi_i = s - n\varrho_i \quad (i = 1, 2),$$
$$d = s^2 + nsc + n^2 b = \xi_1 \xi_2.$$

We shall assume throughout the paper that $d \neq 0$. If $d > 0$, we let Δ denote the open interval $(-2\sqrt{d}, 2\sqrt{d})$, and $\mathscr{A}$ be the set of all totally real algebraic numbers α, all of whose conjugates α_j lie in Δ. Further, we define

$$(1) \qquad g(z) = g_n(z; s) = \big(\xi_2(z - \varrho_1)^n - \xi_1(z - \varrho_2)^n\big)/(\xi_2 - \xi_1),$$

which is monic of degree n in $Q[z]$. We put $\eta = \xi_1/\xi_2$ and $\varkappa = 1$ or 2 according as n is odd or even.

We can now state

THEOREM 2. *Every $\beta \in \mathscr{B}_*$ has minimal polynomial of the form $g(z)$, for some $n \geqslant 3$ and some $s, b, c \in Q$ satisfying $c^2 > 4b$, $d \neq 0$, and*

$$(2) \qquad \eta \notin K^p \text{ for each odd prime } p \mid n, \text{ and, if } n \text{ is even, } d > 0,\ d \notin Q^2.$$

Conversely, given $n \geqslant 3$ and $s, b, c \in Q$ satisfying $c^2 > 4b$, $d \neq 0$, and (2), the polynomial $g(z)$ is irreducible over Q and has all its zeros β_i lying on a circle. Furthermore, $\varkappa$ of these zeros are real, and the centre of the circle has degree $n/\varkappa \geqslant 2$ over Q. So $\beta_i \in \mathscr{B}_*$.

The condition (2) is equivalent to $g(z)$ having a real zero and being irreducible over Q (see Lemma 7). For $\mathscr{B}_n$ we have

THEOREM 3. *Every $\beta \in \mathscr{B}_n$ has minimal polynomial of the form*

$$(3) \qquad P(z) = A \prod_j \big(\xi_2(z - \varrho_1)^{2n} + \xi_1(z - \varrho_2)^{2n} - \alpha_j(z^2 + cz + b)^n\big),$$

for some $\alpha \in \mathscr{A}$, some rational constant A, and some $s, b, c \in Q$ satisfying $c^2 > 4b$, $d > 0$, and (2).

Conversely, given $\alpha \in \mathscr{A}$, $n \geqslant 3$, and $s, b, c \in Q$ satisfying $c^2 > 4b$, $d > 0$, and (2), the polynomial $P(z)$ of (3) is irreducible over Q, and all its zeros β_i are non-real, and lie on the circle $|z - \gamma|^2 = b + c\gamma + \gamma^2$. Here γ is the only real zero of $g(z)$ if n is odd, and the real zero of $g(z)$ further from $-\frac{1}{2}c$ if n is even. So $\beta_i \in \mathscr{B}_n$.

Theorem 3, combined with the earlier results ([1], Theorem 1, and [2] Theorem 3) for circles of totally real centre, immediately gives all circles which contain infinitely many sets of conjugate algebraic numbers. To see this, it is sufficient to remark that no circle with irrational centre can contain infinitely many sets of conjugate quadratic irrationals. Indeed, a simple argument shows that any such circle can contain at most one of these sets.

In these theorems we see that the polynomial $g(z)$ occurs in two different capacities. First of all, when $c^2 > 4b$, $d \neq 0$, and (2) holds, its zeros are elements of $\mathscr{B}_*$. But when (for odd n) also $d > 0$, one real zero of $g(z)$ is the centre of a circle containing elements of $\mathscr{B}_n$.

There is an alternative form of (3) which we used for $n = 3, 4$ in [2]. It is obtained by replacing α by

$$\alpha' = -nc - n^2(c^2 - 4b)/(\alpha - 2s - nc).$$

We shall use this form in the proof of Theorem 1.

The proof of Theorems 2 and 3 occupies the next four sections. Theorem 1 is proved in Section 7. The method we use in the proof of Theorems 2 and 3 is not the same as in [2], which employed automorphic functions. That method can also be used here, though the proof is somewhat longer.

3. Fundamental lemmas. For this section let $\beta \in \mathscr{B}$, and suppose that all the conjugates β_i of β lie on a circle $\mathscr{S}: |z - \gamma|^2 = \Omega$, where γ is not totally real, and of degree n ($\geqslant 3$). So $\beta \in \mathscr{B}_*$ or $\beta \in \mathscr{B}_n$. As was shown in [2], Section 3, $\Omega \in Q(\gamma)$. Taking γ_j ($j = 1, \ldots, n$), with $\gamma_1 = \gamma$, to be the conjugates of γ, and Ω_j the corresponding element of $Q(\gamma_j)$, we define, following [2], the linear transformations Γ_j: $C \cup \{\infty\} \to C \cup \{\infty\}$ by

$$(\Gamma_j z - \gamma_j)(z - \gamma_j) = \Omega_j \quad (j = 1, \ldots, n)$$

or, equivalently,

$$\Gamma_j z = (\gamma_j z + \Omega_j - \gamma_j^2)/(z - \gamma_j) \quad (j = 1, \ldots, n).$$

Put $\Gamma = \Gamma_1$. Note that $\Gamma_j^2 = 1$ ($j = 1, \ldots, n$). Let H denote the group generated by the Γ_j. Since Γ permutes the conjugates of β and $\Gamma\mathscr{S} = \mathscr{S}$, it is easy to show (see [2], Section 3) that every Γ_j also permutes the conjugates of β and that $\Gamma_j\mathscr{S} = \mathscr{S}$. Hence these facts hold for any $\Lambda \in H$.

However, any number $\Omega \epsilon Q(\gamma)$, $\Omega > 0$ can be used to define a circle $\mathscr{S}$, and linear transformations Γ_j, and in this general situation one can prove, using the fact that $\Gamma z = \bar{z}$ if and only if $z \epsilon \mathscr{S}$:

LEMMA 1. *We have* $\Gamma_j \Gamma = \Gamma \bar{\Gamma}_j$ *if and only if* $\Gamma_j \mathscr{S} = \mathscr{S}$.

The details are in [2], Lemma 1.

Returning to our particular situation, we have, from the lemma,

$$\Gamma_j \Gamma = \Gamma \bar{\Gamma}_j \quad (j = 1, \ldots, n). \tag{4}$$

Hence, choosing γ_j non-real, we see that H is non-abelian. Further, since any linear transformation which keeps three elements fixed is the identity, and the elements of H permute the finite set of β_i's, H must be finite (see [2], Lemma 2).

We now need a basic fact:

LEMMA 2. *Any finite non-abelian group of linear transformations which keeps a circle invariant must be dihedral.*

Proof. We use some results from Sections 51–57 of Ford [3] (Theorem 3 in particular). We summarize these results as follows: Any finite non-abelian group of linear transformations is either dihedral, tetrahedral, octahedral or icosahedral. Furthermore, a group of any of the latter three types is conjugate, in the group of all linear transformations, to one of three particular groups G_i^π $(i = 1, 2, 3)$ of linear transformations, obtained in the following way:

Let $\pi\colon S \to C \cup \{\infty\}$ be a stereographic projection from a sphere S in R^3. Then π maps circles on S to circles or straight lines in $C \cup \{\infty\}$. If $\theta\colon S \to S$ is a rotation, then

$$\pi\theta\pi^{-1}\colon C \cup \{\infty\} \to C \cup \{\infty\}$$

is a linear transformation. For any group G of rotations of S, let G^π be the corresponding group of linear transformations. Then, by inscribing a tetrahedron, octahedron or icosahedron in S, the group of all rigid motions which carry this body into itself gives a finite group G_i $(i = 1, 2, 3)$ of rotations of S. This defines G_i^π.

Using these results, we can prove the lemma. Assume that we have a group of linear transformations which keeps a circle invariant, and is conjugate to G_i^π. Then G_i keeps a circle on S invariant. But each of these groups contains two rotations θ, θ' of order > 2, which rotate about different axes, and therefore have different invariant circles. This proves the lemma.

In particular, H is a dihedral group. In fact

LEMMA 3. *The group H is dihedral of order $2n$. Its elements are Γ_j and $\Gamma_j \Gamma$ $(j = 1, \ldots, n)$.*

Proof. Applying an automorphism σ of $Q(\gamma, \gamma_2, \ldots, \gamma_n)$ which takes γ to γ_i, we obtain, from (4) with $\gamma_j = \sigma^{-1}\gamma_k$,

$$\Gamma_k \Gamma_i = \Gamma_i \Gamma_h \quad (i, k = 1, \ldots, n), \tag{5}$$

where h depends on i and k, and $h \neq k$ if γ_j is non-real. This shows that no Γ_i belongs to the centre of H. It also shows that $\Gamma_i \Gamma_k \Gamma_i = \Gamma_h$, so (as H is generated by the Γ_i) every conjugate of Γ_k is of the form Γ_h for some h.

Suppose that H is dihedral of order $2m$. We must show that $m = n$. The second assertion of the lemma then follows easily.

Consider first the case m odd. Then all m involutions of H are conjugate. Hence the Γ_j are the only involutions of H, and $m = n$.

Now take m even. Then the m non-central involutions divide into two conjugacy classes. Since any conjugacy class containing some Γ_j contains only elements of the form Γ_k, it follows that either $m = n$ if there are Γ_j's in both conjugacy classes, or $m = 2n$ if all Γ_j's lie in one conjugacy class. The latter possibility cannot occur, because in that case all the Γ_j would belong to a subgroup of index 2 in H. This completes the proof.

We now quote Lemma 4 from [2]. It is clear from the preceding argument that the hypotheses of this lemma are satisfied. So we have the following results:

LEMMA 4. (i) *There exist rational numbers b, c such that $\Omega = b + c\gamma + \gamma^2$.*

(ii) *The roots ϱ_1, ϱ_2 of the equation $x^2 + cx + b = 0$ are real and unequal, and are inverse with respect to the circle $\mathscr{S}$.*

(iii) *Each Γ_j interchanges ϱ_1 and ϱ_2, so that ϱ_1 and ϱ_2 are fixed points of $\Gamma_j \Gamma$ $(j = 1, \ldots, n)$.*

(iv) *The fixed points of Γ_j lie on $\mathscr{S}$.*

We can now show

LEMMA 5. *The minimal polynomial of γ is of the form $g(z)$, where b, c are as above and $s = \sum_{j=1}^{n} \gamma_j$. Further $d > 0$.*

Proof. Define the linear transformation L by

$$Lz = (z - \varrho_1)/(z - \varrho_2). \tag{6}$$

Then $T_j = L\Gamma_j \Gamma L^{-1}$ $(j = 1, \ldots, n)$ has fixed points 0 and ∞, so that $T_j z$ is of the form $\lambda_j z$ for some $\lambda_j \epsilon C$. But $T_j^n = 1$, so λ_j is an nth root of unity. Further the λ_j are all distinct, so we can relabel the γ_j so that $\lambda_j = \omega^{j-1}$ $(j = 1, \ldots, n)$, where $\omega = \exp(2\pi i/n)$.

Putting $\mu = L\gamma$, we have

$$L\gamma_j = L\Gamma_j L^{-1} 1 = T_j L\Gamma L^{-1} 1 = T_j \mu = \omega^{j-1}\mu \quad (j = 1, \ldots, n). \tag{7}$$

Writing $G(Z) = \prod_{j=1}^{n}(Z - L\gamma_j)$, we thus deduce $G(Z) = Z^n - \mu^n$. Putting $Z = Lz$ and noting that $g(z)$ is monic, we obtain

$$g(z) = \big((z-\varrho_1)^n - \mu^n(z-\varrho_2)^n\big)/(1-\mu^n).$$

Since the coefficient of z^{n-1} equals $-s$, we easily find that

$$\mu^n = \xi_1/\xi_2 = \eta, \tag{8}$$

which gives (1). As regards the assertion $d > 0$, see Lemma 6 (iii), (iv) below.

For future reference, we note that

$$LT_jL^{-1}z = \omega^{j-1}\mu/z \qquad (j = 1, \ldots, n). \tag{9}$$

This follows easily from (7) and the fact that LT_jL^{-1} interchanges 0 and ∞.

4. The polynomial $g(z)$. We now take a closer look at $g(z)$, defined by (1) for $n \geqslant 3$ and any $s, b, c \in Q$ with $c^2 > 4b$ and $d \neq 0$. Let $\gamma_1 = \gamma, \ldots, \gamma_n$ be its zeros. Define L by (6). The condition $d \neq 0$ is no essential restriction, because for $d = 0$ the polynomial takes the degenerate form $g(z) = (z-\varrho_i)^n$ $(i = 1$ or $2)$.

LEMMA 6. (i) *The numbers s, b, c are uniquely determined by $g(z)$.*

(ii) *The zeros of $g(z)$ all lie on a circle, provided $s \neq -\frac{1}{2}nc$.*

(iii) *The zeros of $g(z)$ are all distinct. Exactly 1, 0, or 2 of them are real according as n is odd, n is even and $d < 0$, or n is even and $d > 0$.*

(iv) *If n is odd and γ is the real zero of $g(z)$, then $b + c\gamma + \gamma^2 > 0$ if and only if $d > 0$.*

(v) *If n is even and $d > 0$, then $b + c\gamma + \gamma^2 > 0$ for precisely one choice of γ as a real zero of $g(z)$, namely that one which is further from $-\frac{1}{2}c$.*

Proof. (i) Calculating the first few coefficients of $g(z)$, we get

$$g(z) = z^n - sz^{n-1} - \tfrac{1}{2}(n-1)s'z^{n-2} - \tfrac{1}{6}(n-1)(n-2)s''z^{n-3} - \ldots,$$

where

$$s' = sc + nb, \qquad s'' = s(c^2 - b) + nbc.$$

Then

$$d = s^2 + ns', \qquad b = (s'^2 - ss'')/d, \qquad c = (ss' + ns'')/d,$$

whence the result.

(ii) Obviously, the $L\gamma_j$ are the roots of $z^n = \eta$, and so all lie on a circle of centre 0. But L^{-1} maps any such circle, except the unit circle, to a circle. Since η is real and $\neq 1$, the exceptional case occurs for $\eta = -1$, which implies $s = -\frac{1}{2}nc$.

(iii) Since the $L\gamma_j$ are all distinct, so are the γ_j. As L maps the real axis into itself and $\operatorname{sgn}\eta = \operatorname{sgn}d$, the latter assertion follows readily.

(iv) If n is odd, we have, using the fact that $b + c\gamma + \gamma^2 = (\gamma - \varrho_2)^2 L\gamma$,

$$b + c\gamma + \gamma^2 > 0 \Leftrightarrow L\gamma > 0 \Leftrightarrow \eta > 0 \Leftrightarrow d > 0.$$

(v) Suppose that n is even and that $d > 0$. Now $g(z)$ has two real zeros γ, γ', say. We have $L\gamma' = -L\gamma$. The choice is determined by the condition $L\gamma > 0$. From (6) we see that γ and γ' lie outside and inside the interval (ϱ_1, ϱ_2), respectively. The result follows easily.

LEMMA 7. *The polynomial $g(z)$ has a real zero and is irreducible over Q if and only if (2) holds. If this is the case, then its zeros lie on a circle whose centre has degree $n/\varkappa$ over Q.*

Proof. By Lemma 6 (iii), $g(z)$ has a real zero if and only if $d > 0$ for even n. We therefore assume that this condition is satisfied.

Suppose first that $\eta = \varphi^p$, where p is an odd prime divisor of n and $\varphi \in K$. Then

$$h(z) = \big((z-\varrho_1)^{n/p} - \varphi(z-\varrho_2)^{n/p}\big)/(1-\varphi)$$

divides $g(z)$, so that $g(z)$ has a zero of degree $\leqslant 2n/p < n$ over Q, whence $g(z)$ is reducible over Q. (It is in fact easy to see that $h(z) \in Q[z]$.)

Next let n be even and $\sqrt{d} \in Q$. Then

$$\big(\sqrt{d}\,(z-\varrho_1)^{n/2} - \xi_1(z-\varrho_2)^{n/2}\big)/(\sqrt{d} - \xi_1)$$

belongs to $Q[z]$ and divides $g(z)$.

Conversely, let $g(z)$ be reducible over Q. We contend that (2) does not hold. Let $h(z)$ be a proper monic divisor of $g(z)$ in $Q[z]$. By relabelling the γ_j, we may suppose that $\gamma_1, \gamma_2, \ldots, \gamma_m$ $(1 \leqslant m < n)$ are the zeros of $h(z)$. Multiplying the equations $(L\gamma_j)^n = \eta$ $(j = 1, \ldots, m)$, we obtain, by (6),

$$\big(h(\varrho_1)/h(\varrho_2)\big)^n = \eta^m.$$

Let $k = (m, n) = um + vn$, say. Writing $\tau_i = h(\varrho_i)^u \xi_i^v$ $(i = 1, 2)$, we get $\eta^k = (\tau_1/\tau_2)^n$, whence

$$\eta = \pm(\tau_1/\tau_2)^{n/k}. \tag{10}$$

If an odd prime p divides n/k, then $\eta \in K^p$, and we are finished. Suppose therefore that $n/k = 2^r$. Now $d > 0$ implies $\eta > 0$, so that we must have the plus sign in (10). Hence $\xi_1/\tau_1^{2^r} = \xi_2/\tau_2^{2^r} = r$, say, where r is rational. So $d = r^2(\tau_1\tau_2)^{2^r} \in Q^2$, and the proof of the first part is complete.

For the second part, let $g(z)$ be irreducible and have a real zero γ. By Lemma 6 (ii), the zeros of $g(z)$ lie on a circle $\mathscr{S}_*$, because the exceptional case $s = -\frac{1}{2}nc$ leads to $\eta = -1$, which contradicts (2). Since L maps $\mathscr{S}_*$ to $|z| = |L\gamma|$, we find that

$$\gamma_* = \tfrac{1}{2}\big(\gamma + L^{-1}(-L\gamma)\big) = (\gamma^2 - b)/(2\gamma + c)$$

is the centre of $\mathscr{S}_*$. So $[Q(\gamma):Q(\gamma_*)] \leqslant 2$. Thus $\deg \gamma_* = n$ if n is odd. Suppose that n is even. Then $\gamma' = L^{-1}(-L\gamma)$ is a conjugate of γ (cf. the proof of Lemma 6 (v)). Clearly $\gamma_* = (\gamma'^2 - b)/(2\gamma' + c)$. So γ_* has less than n conjugates, whence $\deg \gamma_* = \frac{1}{2}n$. This completes the proof.

5. Proof of Theorem 3. Let $\beta \in \mathscr{B}_n$ $(n \geqslant 3)$, and put $\gamma = \gamma(\beta)$. Then by Lemma 5, γ has minimal polynomial of the form $g(z)$ for some $s, b, c \in Q$ with $c^2 > 4b$, $d > 0$. By Lemma 4, the circle $\mathscr{S}$ on which the conjugates of β lie has the equation $|z-\gamma|^2 = \Omega$, where $\Omega = b + c\gamma + \gamma^2$. Now define

$$\alpha_j = \xi_2 (L\beta_j)^n + \xi_1 (L\beta_j)^{-n} \tag{11}$$

for each conjugate β_j of β. From the fact that $\Omega = (\gamma - \varrho_1)(\gamma - \varrho_2)$, we see that

$$|L(\gamma \pm \sqrt{\Omega})| = |\gamma \pm \sqrt{\Omega} - \varrho_1| / |\gamma \pm \sqrt{\Omega} - \varrho_2| = (L\gamma)^{1/2} = \mu^{1/2}, \tag{12}$$

so that L maps the circle $\mathscr{S}$ to the circle $|z|^2 = \mu$. It now follows easily, by (8), that for z on $\mathscr{S}$, $\xi_2 (Lz)^n + \xi_1 (Lz)^{-n}$ is real and lies on the closed interval $[-2\sqrt{d}, 2\sqrt{d}]$. Hence $\alpha_j \in [-2\sqrt{d}, 2\sqrt{d}]$. We relabel the β_j so that $\alpha_1, \ldots, \alpha_t$ are distinct and form a complete set of conjugates. Define a monic polynomial $P(z)$ by (3), where j ranges from 1 to t. It is then clear, by (11) and (6), that the minimal polynomial of β divides $P(z)$.

To show that $P(z)$ is irreducible, we look first at the equation

$$\alpha = \xi_2 z^n + \xi_1 z^{-n} \quad \text{or} \quad z^{2n} - (\alpha/\xi_2) z^n + \eta = 0,$$

for any complex value of α. The roots of this equation are clearly $\omega^{i-1} z_0$ and $\omega^{i-1} \mu / z_0$ $(i = 1, \ldots, n)$, where z_0 is one root. Hence, by (9), these roots can also be written as $L\Gamma_i \Gamma L^{-1} z_0$ and $L\Gamma_i L^{-1} z_0$ $(i = 1, \ldots, n)$. Hence, replacing z by Lz, we see that the roots of $\alpha = \xi_2 (Lz)^n + \xi_1 (Lz)^{-n}$ are $\Gamma_i \Gamma z_0$ and $\Gamma_i z_0$ $(i = 1, \ldots, n)$, where z_0 is one root. Since the Γ_i permute the conjugates of β (see Section 3), it follows that, for $j = 1, \ldots, t$, the roots of

$$\alpha_j = \xi_2 (Lz)^n + \xi_1 (Lz)^{-n} \tag{13}$$

are all conjugates of β_j, and hence of β. If these roots are all distinct for every $j = 1, \ldots, t$, the result follows. If not, then some β_k is a fixed point of some Γ_i, i.e. $\Gamma_i \beta_k = \beta_k$. In a suitable normal extension of Q, apply an automorphism which maps γ_i to γ. Then we obtain $\Gamma \beta_h = \beta_h$ for some h. But now $\beta_h = \gamma \pm \sqrt{\Omega}$ is real, which contradicts the hypothesis.

From the fact that the roots of (13) are distinct, it also clearly follows that $\alpha_j \neq \pm 2\sqrt{d}$, so that $\alpha_j \in \mathscr{A}$. This proves the first part of Theorem 3.

To prove the converse part, let $n \geqslant 3$, and $s, b, c \in Q$ satisfying $c^2 > 4b$, $d > 0$ and (2), and some $\alpha \in \mathscr{A}$ be given. Then by Lemmas 6 and 7, $g(z)$ is irreducible, and has a unique real zero γ with $\Omega = b + c\gamma + \gamma^2 > 0$,

as specified in Lemma 6 (iv), (v). Using (6), it is easy to deduce (8) from $g(\gamma) = 0$. From (12) we infer that L maps $\mathscr{S}$: $|z-\gamma|^2 = \Omega$ to the circle $|z|^2 = \mu$.

Now consider the equation $z^{2n} - (\alpha_j/\xi_2) z^n + \eta = 0$, for any conjugate α_j of α. Since $\alpha_j \in \Delta = (-2\sqrt{d}, 2\sqrt{d})$, all roots of this equation lie on $|z|^2 = \mu$, and none of them is real. Applying the transformation L^{-1}, we see that the roots of (13) lie on $\mathscr{S}$, and so, defining $P(z)$ by (3), all zeros of $P(z)$ are non-real and lie on $\mathscr{S}$. By the remark made in Section 2, at least one zero of $P(z)$ has degree $\geqslant 3$ over Q, and so belongs to $\mathscr{B}_n$. Then since (Lemma 6 (i)) the parameters s, b, c are determined by γ, we see from the first part of the theorem that $P(z)$ is irreducible over Q. This completes the proof of Theorem 3.

6. Proof of Theorem 2. Let $\beta \in \mathscr{B}_*$. Consider first the case when $\gamma = \gamma(\beta)$ is not totally real. Let s, b, c be the parameters connected with γ, given by Lemma 5. Let $g_*(z)$ denote the minimal polynomial of β. From the argument in the preceding section it follows that $g_*(z) | P(z)$, where $P(z)$ is formed with $\alpha_j = \pm 2\sqrt{d}$ (either sign or both signs according as $d \in Q^2$ or $d \notin Q^2$). Moreover, it is easily seen that each root of (13) is now repeated twice, whence the argument gives $P(z) = g_*(z)^2$.

For $d \in Q^2$, $\alpha_1 = 2\varepsilon\sqrt{d}$ $(\varepsilon = \pm 1)$, we then have

$$g_*(z) = \big((z-\varrho_1)^n - \varepsilon\sqrt{\eta}\,(z-\varrho_2)^n\big)/(1 - \varepsilon\sqrt{\eta}),$$

as is easily verified by squaring. So $g_*(z) = g_n(z; s + \delta\sqrt{d})$ for $\delta = \varepsilon \operatorname{sgn} \xi_1$, because

$$(s + \delta\sqrt{d} - n\varrho_1)/(s + \delta\sqrt{d} - n\varrho_2) = \big(\xi_1 + \delta(\xi_1\xi_2)^{1/2}\big)/\big(\xi_2 + \delta(\xi_1\xi_2)^{1/2}\big) = \varepsilon\sqrt{\eta}.$$

If $d \notin Q^2$, then $g_*(z)$ is a product of the above polynomials with $\varepsilon = \pm 1$, and so we get

$$g_*(z) = \big(\xi_2 (z-\varrho_1)^{2n} - \xi_1 (z-\varrho_2)^{2n}\big)/(\xi_2 - \xi_1) = g_{2n}(z; 2s).$$

Hence $g_*(z)$ is of the form (1) with the parameters n, s replaced by either $n, s + \delta\sqrt{d}$ or $2n, 2s$. With the corresponding new values for η and d, (2) then holds, by Lemma 7, and so the first assertion of Theorem 2 is true, for $\gamma(\beta)$ not totally real.

Now let $\beta \in \mathscr{B}_*$, with $\gamma = \gamma(\beta)$ totally real. Then β is of degree 4, and is given in [1], equation 10 (ii), p. 342. (Equation 10 (i) is not relevant here, as $\deg \beta \geqslant 3$.) Using the notation of [1], we have that β is of the form $\beta = \gamma_j \pm \Omega_j^{1/2}$ ($j = 1$ or 2), where $\gamma = \gamma_1$ is real quadratic with conjugate γ_2, γ_3 is a rational number such that γ_3 lies between γ and γ_2, and $\Omega_i = (\gamma_i - \gamma_j)(\gamma_i - \gamma_k)$ for any permutation i, j, k of 1, 2, 3. Take $\varrho_1, \varrho_2 = \gamma_3 \pm \Omega_3^{1/2}$, and define $s = 2\gamma_1 + 2\gamma_2$, $b = \varrho_1\varrho_2$, $c = -\varrho_1 - \varrho_2 = -2\gamma_3$. It is then easy to check that the minimal polynomial of β is $g_4(z; s)$. Clea-

rly, $c^2 > 4b$ and $d \neq 0$. Finally, Lemma 7 shows that (2) holds. This completes the proof of the first part of Theorem 2. The converse part is an immediate consequence of Lemmas 6 and 7.

7. Proof of Theorem 1. For the proof, it will be sufficient to show the following result, which is in fact a generalization of an example in [2] (Section 11, Example 3).

LEMMA 8. *Let $n \geqslant 3$, $b = 0$, $c = 1$, $s = S/q$, where S and q are positive integers such that $(S, q) = 1$ and $S \geqslant n^2q^2$. Then the corresponding polynomial*

$$g(z) = z^n - (S/nq)\left((z+1)^n - z^n\right)$$

is irreducible, and has a real zero γ such that the circle $|z-\gamma|^2 = \gamma+\gamma^2$ contains infinitely many sets of conjugate algebraic integers.

Proof. We have $\varrho_1 = -1$, $\varrho_2 = 0$, $d = s^2+ns > 0$, $\eta = (S+nq)/S$. Suppose that $\eta \in Q^k$ for some natural number $k \geqslant 2$. Put $r = (S, n)$. Then $S = ru^k$, $S+nq = rv^k$, for some natural numbers u, v. But now

$$S+nq \geqslant r(u+1)^k > S+rku^{k-1} \geqslant S+2ru^{k/2} = S+2r^{1/2}S^{1/2} > S+nq,$$

which is impossible. Hence $\eta \notin Q^k$ for $k \geqslant 2$ and also $d = \xi_2^2\eta \notin Q^2$. Thus (2) holds, so that $g(z)$ is irreducible. It has a unique real zero γ with $\gamma+\gamma^2 > 0$.

From Theorem 3, it remains only to show that there are infinitely many $\alpha \in \mathcal{A}$ such that the polynomial $P(z)$ has integral coefficients. For our example, $P(z) = \prod_j P_j(z)$, where

$$P_j(z) = \left(s(z+1)^{2n} + (s+n)z^{2n} - a_j(z^2+z)^n\right)/(2s+n-a_j).$$

It is convenient here to change variables, and put

$$a_j' = (na_j - 2ns)/(-a_j+2s+n).$$

(Cf. the remark at the end of Section 2.) Then $-a_j'$ is the coefficient of z^{2n-1} in $P_j(z)$. It is easy to check that $a_j \in \Delta$ is equivalent to $a_j' \in \Delta'$, where $\Delta' = (2s-2\sqrt{d},\ 2s+2\sqrt{d})$. Then substituting for

$$a_j = \left((2s+n)a_j' + 2ns\right)/(a_j'+n)$$

in $P_j(z)$, we get

$$P_j(z) = (z^2+z)^n + (a_j'+n)n^{-2}\left(s(z+1)^n - (s+n)z^n\right)\left((z+1)^n - z^n\right).$$

But now Δ' has length $4\sqrt{d} > 4s \geqslant 4n^2q$, so (see e.g. [2], Lemma 21) we can choose infinitely many α' of the form $\alpha' = n^2q\theta - n$, where θ is an algebraic integer, such that all the conjugates of α' lie in Δ'. If a_j' is of this form, then the coefficients of $P_j(z)$ are algebraic integers. Thus each θ gives a set of conjugate algebraic integers on $|z-\gamma|^2 = \gamma+\gamma^2$, and hence the proof of Lemma 8 is complete.

Note added in proof. We would like to thank J. H. Conway for pointing out the following simple proof of Lemma 2: Let $N = \deg\beta$. Since each $A \in H$ permutes the conjugates of β, it is easy to see that H is isomorphic to a subgroup of the symmetric group on N symbols. Further, as each $A \in H$ preserves (or reverses) the order of the β_i on $\mathscr{S}$, H must be a dihedral group.

References

[1] V. Ennola, *Conjugate algebraic integers on a circle with irrational center*, Math. Zeitschr. 134 (1973), pp. 337–350.

[2] V. Ennola and C. J. Smyth, *Conjugate algebraic numbers on a circle*, Ann. Acad. Sci. Fennicae A I 582 (1974).

[3] L. R. Ford, *Automorphic Functions*, 2nd ed., Chelsea, 1951.

[4] R. M. Robinson, *Conjugate algebraic integers on a circle*, Math. Zeitschr. 110 (1969), pp. 41–51.

UNIVERSITY OF TURKU
Finland

Received on 30. 5. 1974 (576)